Intelligence Community (IC) Security DTD

Version 1 - Draft

Presented by:

Mary Ann Melosh

of

Science Applications International Corporation
An Employee-Owned Company

Supporting the Intelink Management Office

2 November, 2000

© 2000 SAIC, All Rights Reserved

Overview

- **The purpose of Intelligence Community (IC) Security Document Type Definition (DTD) is to provide a common set of XML elements (TAGS) for implementing security-based metadata throughout the IC**
- **IC Security DTD may be incorporated into organizational XML-based DTDs by calling the entity declaration referenced within the core IC Security DTD**

© 2000 SAIC, All Rights Reserved

Overview (Continued)

- It is intended to provide a basic structure for incorporating security metadata into XML documentation
- It is not intended to address all business rules associated with using security metadata
- The IC Security DTD is designed around the CAPCO security markings specification and other related sources, capturing the security classification, control markings, and dissemination controls

Note: Controlled Access Program Coordination Office (CAPCO) Authorized Classification and Control Markings Register

© 2000 SAIC, All Rights Reserved

IC Security DTD Background

- **SAIC's initial involvement was in support of the CIA/DI/OSS for the SGML/XML Authoring Prototype**
- **iWeb initiative to move the DI's current production processes toward a web based publishing and dissemination system.**
- **XML identified by iWeb as a possible enabling technology.**
- **We were to implement the same standard that the existing DI/OSS MS Office Program Team used in development of the IC Classification Macro for Word**

© 2000 SAIC, All Rights Reserved

IC Security DTD Background

- **Contacted Agency Metadata Working Group for clarifications which resulted in participation on IC Metadata Workshops**
- **Began coordination with IMO who had announced that they would expand the Intelink Metadata Standard to include fields in the CIA Metadata Standard**
- **During workshops, interfaced with NGIC who had also implemented a similar security model**
- **Intelink IMD will host all releases in softcopy**

© 2000 SAIC, All Rights Reserved

IC Security DTD Background (Continued)

- **Collaborated together for several sessions and e-mails over a few months to develop a common model which would not be CIA or NGIC specific but one that the entire IC Community could use**
- **Under separate support task for the IMO, SAIC was requested to send it to JICPAC for preliminary review due to their experience with SGML in a production environment**
- **Presented it at the Intelink Conference in Monterey late September**
- **Provided an informal brief to the CAPCO Working Committee 19 October**
- **Provided briefing to the JIVA SAG 23 October**
- **Continue to seek input from other organizations as well as approval from the CAPCO Working Committee**

© 2000 SAIC, All Rights Reserved

IC Security DTD Version 1 - Draft: Modifications & Maintenance

- **NOTE:**
  - We know there are already a couple elements which have just recently been removed per CAPCO which are still included in the DTD.
  - There are a couple elements which are commented as CIA specific. We will remove them and place them in a CIA-specific Security Mod and will provide samples of how other organizations can do the same.

    EX: AIUO - Administrative Internal Use Only
- **MAINTENANCE:**
  - The DTD will require modifications as CAPCO releases updates to the CAPCO standard.

© 2000 SAIC, All Rights Reserved

What we learned

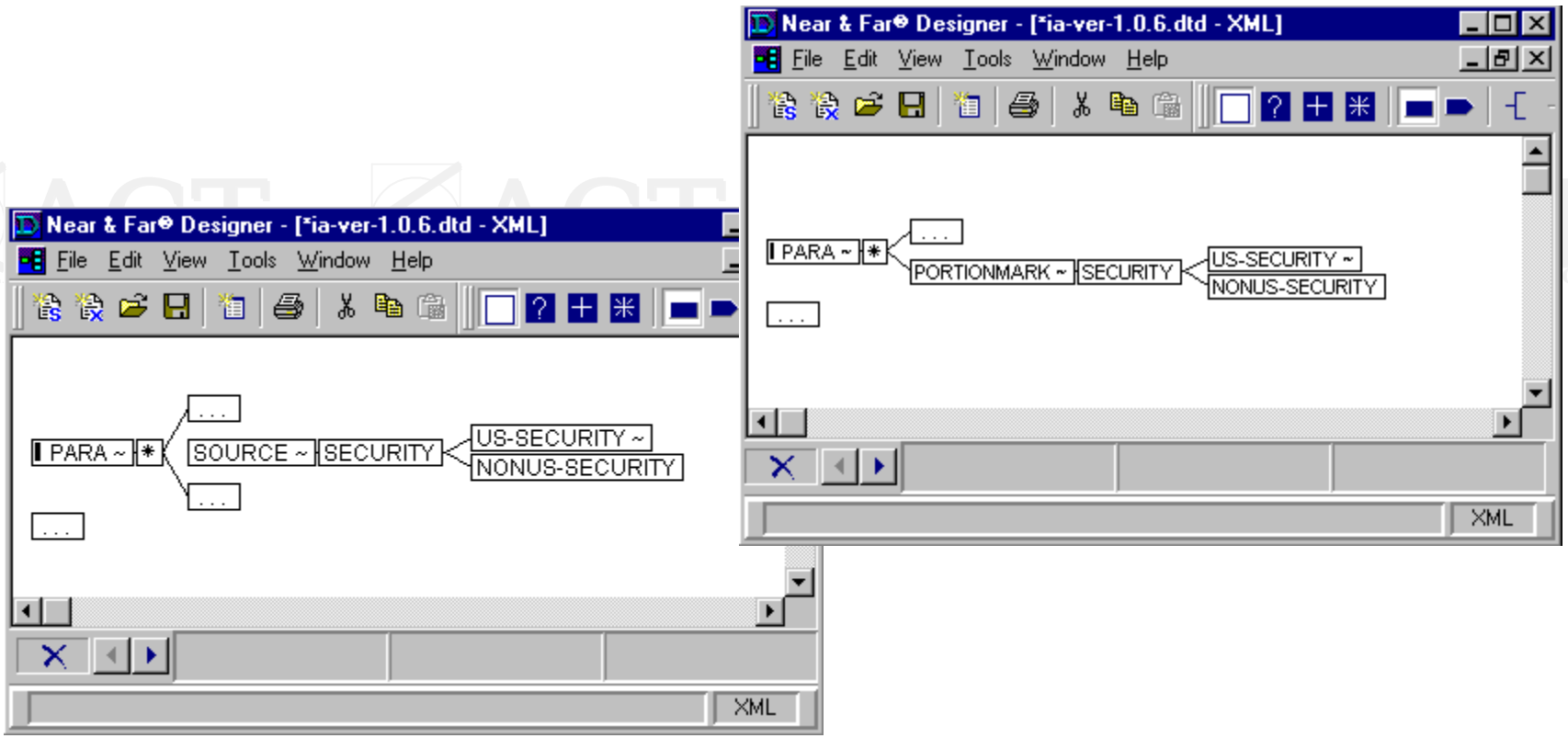
- The security model could be implemented many ways
- Most ways could be 'correct' implementations
- Traditionally think of element / attribute

  Class (U | C | S | TS)
- To fully implement CAPCO, the model is several levels deep
- Cannot have multi-level attributes
- Elements can also be the data.
  - Empty elements are used in many cases. The element is simply selected and other user input is not required. Ensures completeness and accuracy
  - The tags are the information - regardless of how XML instance is formatted for display, underlying data is unaffected and preserved.

© 2000 SAIC, All Rights Reserved

IC Security DTD Version 1 - Draft: Implementation Scenarios

Possible Use of Security Model Within Organizational XML-based DTDs

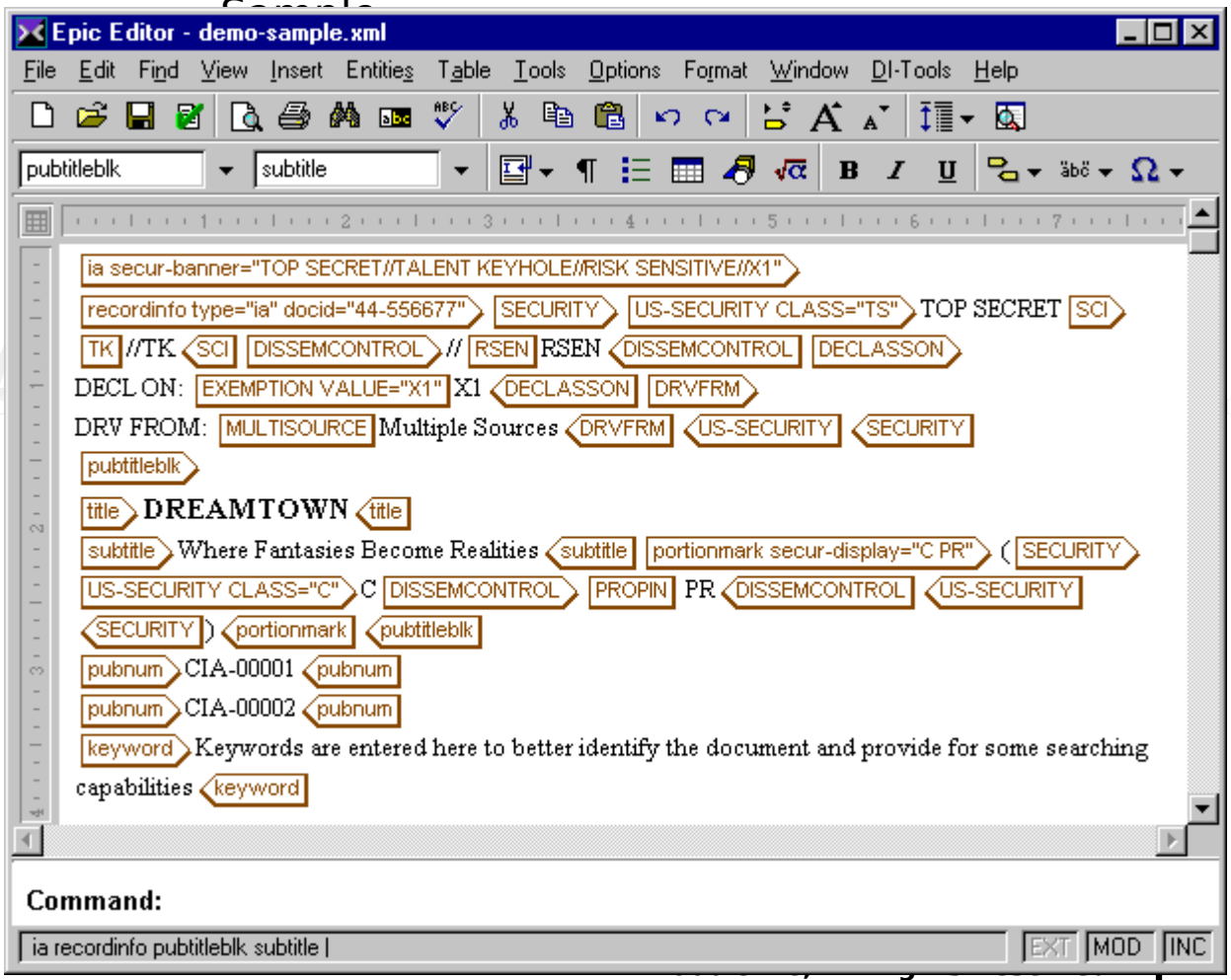


© 2000 SAIC, All Rights Reserved

IC Security DTD Version 1 - Draft: Sample Instance

- **Added attributes for displaying security portion marks and banners**
- **Values of the security elements and attributes interrogated to develop a proper text string and output the result, using a programming language to do the calculations**
- **When transforming to HTML utilizing XSL-T, the rollup has already been done and can be reused without extensive**

Tagged View - Unclassified



IC Security DTD Version 1 - Draft: Sample Instance

ASCII View

Unclassified Sample

demo-sample.xml - Notepad

File Edit Search Help

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE ia PUBLIC "DI/OSS//DTD IA Version 1.0.6, dated 01 September 2000//EN"
<!--ArborText, Inc., 1988-2000, v.4002-->
]>
<ia secur-banner="TOP SECRET//TALENT KEYHOLE//RISK SENSITIVE//X1">
<recordinfo type="ia" docid="44-556677">
<SECURITY><US-SECURITY CLASS="TS">
<SCI><TK/></SCI>
<DISSEMCONTROL><RSEN/></DISSEMCONTROL>
<DECLASSON><EXEMPTION VALUE="X1"/></DECLASSON>
<DRVFRM><MULTISOURCE/></DRVFRM>
</US-SECURITY>
</SECURITY>
<pubtitleblk>
<title>DREAMTOWN</title>
<subtitle>Where Fantasies Become Realities</subtitle>
<portionmark secur-display="C PR"><SECURITY><US-SECURITY CLASS="C">
<DISSEMCONTROL><PROPIN/></DISSEMCONTROL>
</US-SECURITY>
</SECURITY>
</portionmark>
</pubtitleblk>
<pubnum>CIA-00001</pubnum>
<pubnum>CIA-00002</pubnum>
<keyword>Keywords are entered here to better identify the document and provide
for some searching capabilities</keyword>
```


© 2000 SAIC, All Rights Reserved

Thank You

- **Mary Ann Melosh**
  - 1710 SAIC Drive
    T2-5-1
    McLean, Virginia 22102
  - (703) 676-5826
  - meloshm@saic.com

ACT APPLIED CONTENT TECHNOLOGIES

© 2000 SAIC, All Rights Reserved